POC Radius, rapport mise en service

Table des matières

User Story 7

En tant que responsable de la sécurité, je veux qu'uniquement les flux identifiés (dans l'exercice précédent sur la DMZ ainsi que les nouveaux flux identifiés dans cet exercice) soit autorisé à traverser le routeur, dans le but de protéger l'infrastructure d'accès non autorisés. Dessiner les divers flux sur le schéma

Tests d'acceptation :

Schéma des flux et tableau des actions

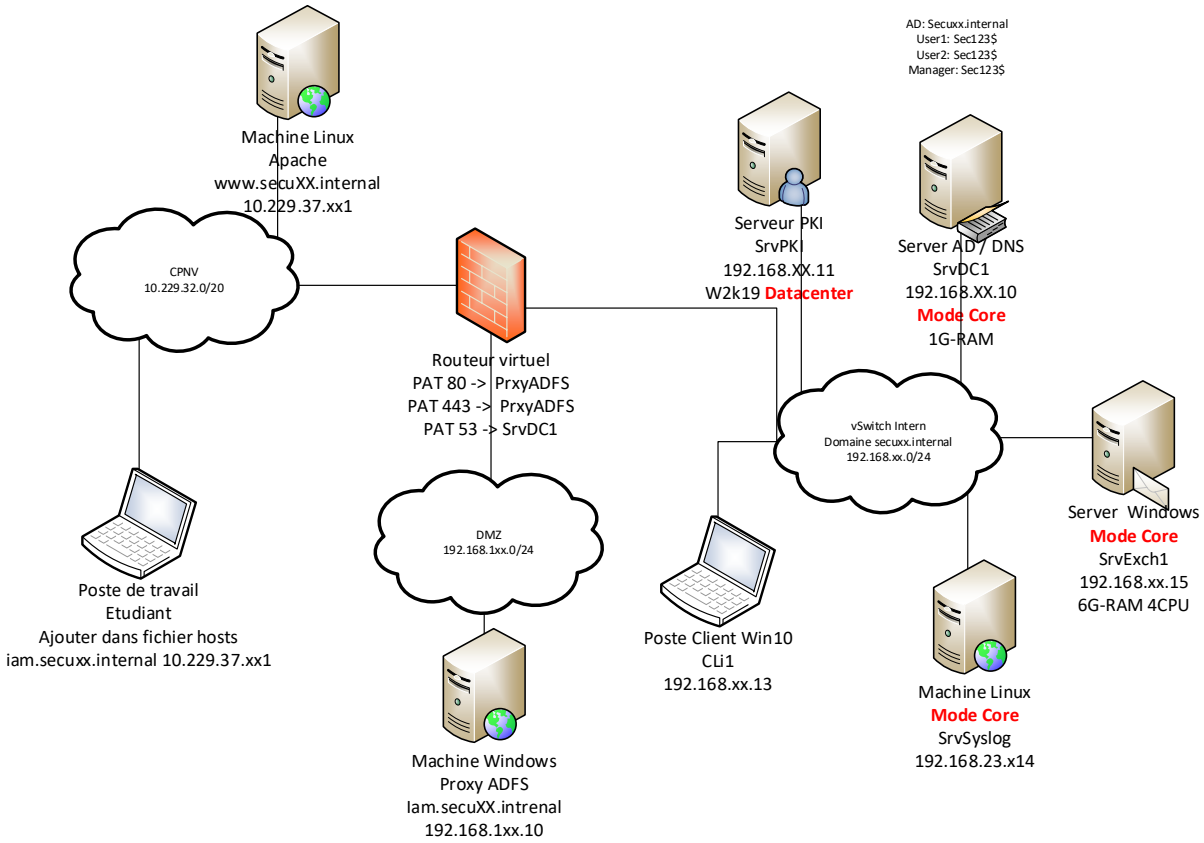


Tableau des actions :

Source	Destination	Protocol	Action

Image avec les règles du firewall, (onglet Filter Rules de IP Firewall sur Winbox), mettez des commentaires dans les règles afin d'éclaircir la lecture

Test d'accès à Internet en direct (sans proxy) :

Image doit montrer que ce n'est pas possible, par exemple un wget en powershell vers un site externe non autorisé

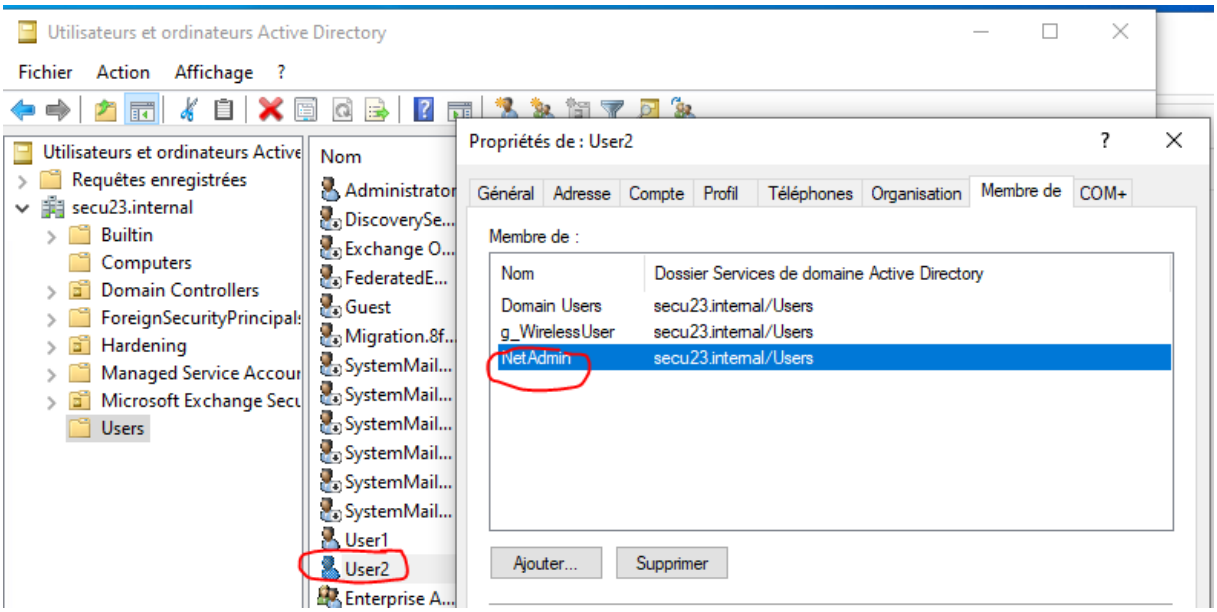
Test d'accès à Internet par le proxy

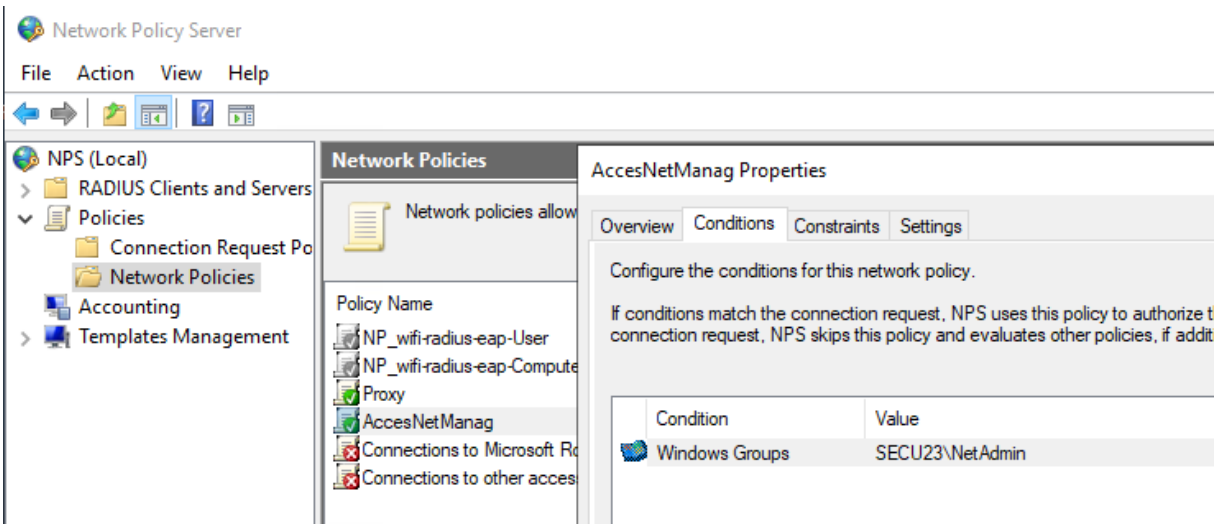
Image doit montrer que c'est possible à l'aide du proxy sur le site vd.ch par exemple

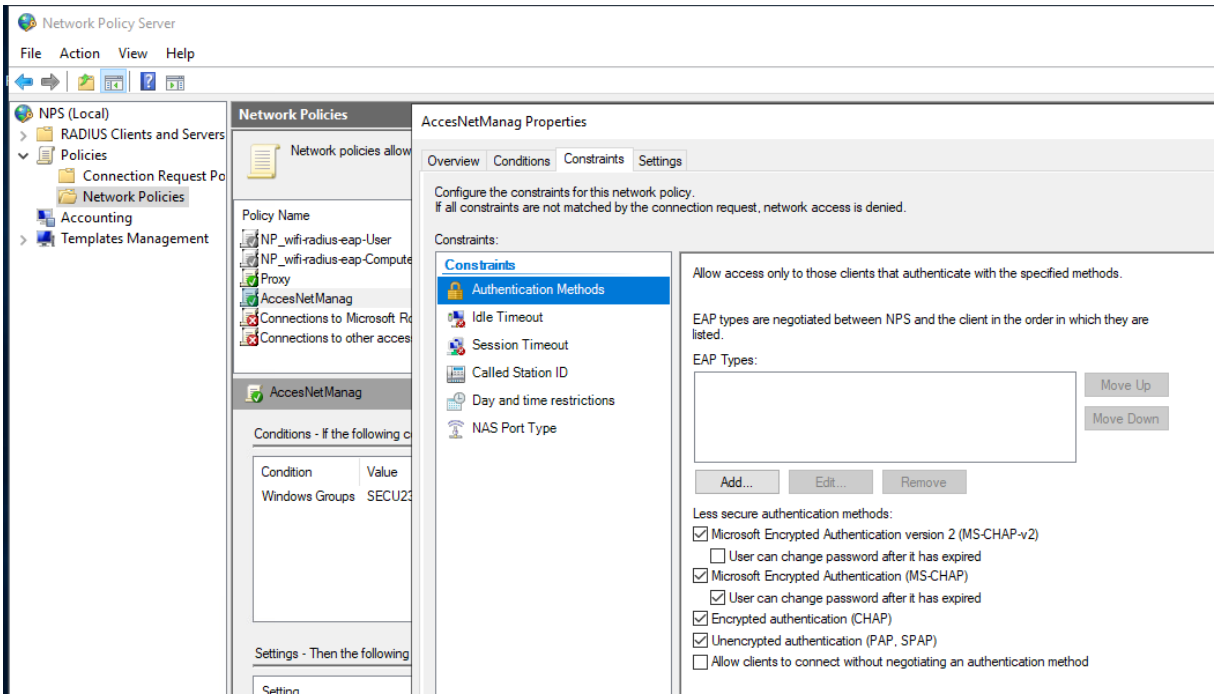
User Story 8

En tant que responsable de la sécurité, je veux que l'ensemble de mon routeur (Mikrotik) puisse être consulté en lecture seul par les utilisateurs du groupe secu_net_admin par l'utilisation d'un protocole AAA, dans le but d'accroitre la sécurité et la granularité des accès.

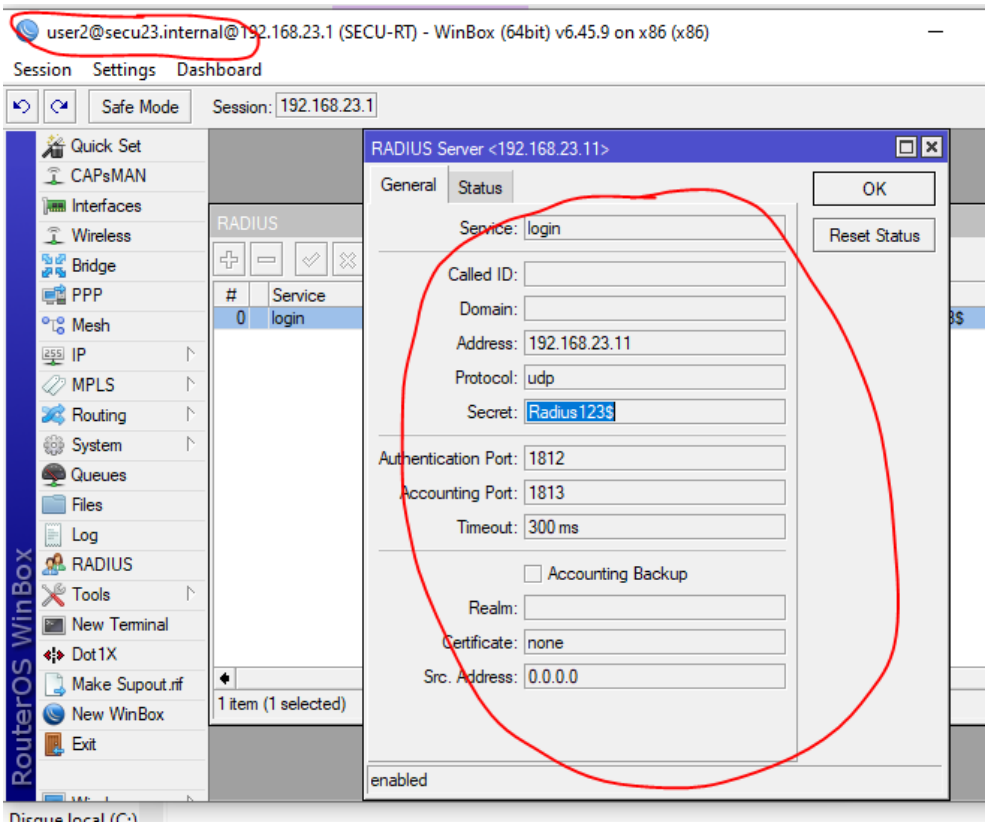
Tests d'acceptation :





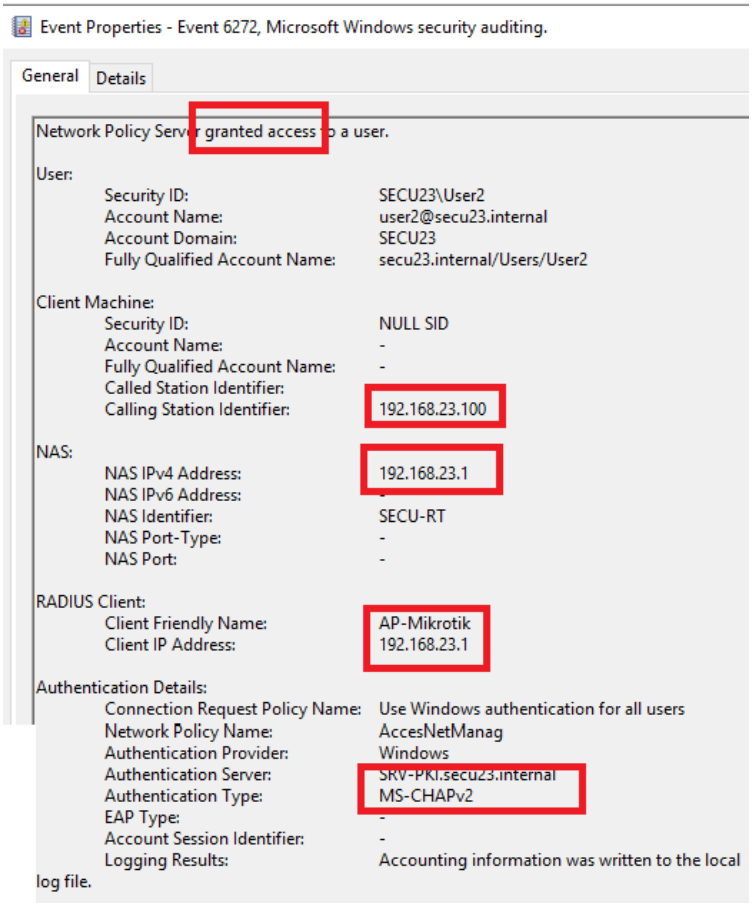


Authentification



On voit que tous les paramètres sont grisés donc on est en read only

Log de radius pour le login sur le Mikrotik

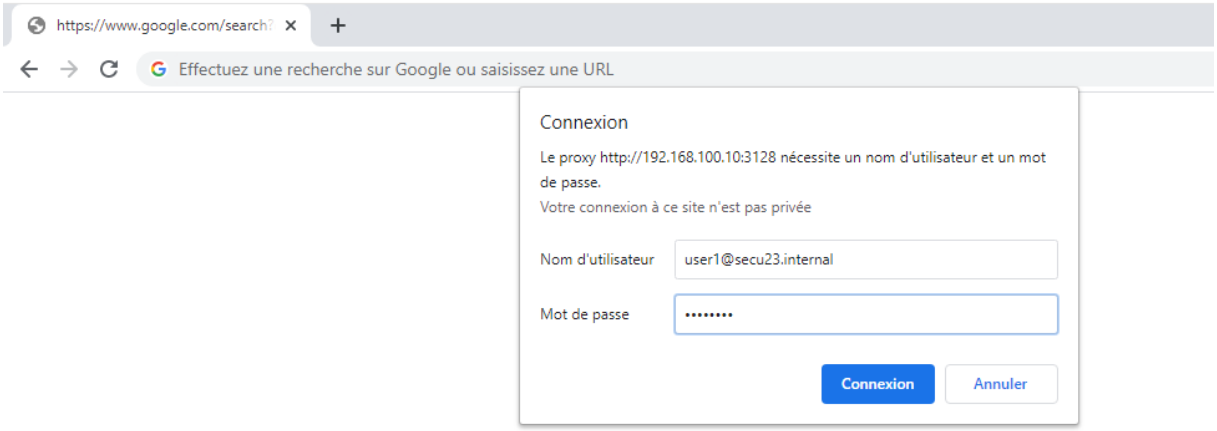


User Story 9

En tant que responsable de la sécurité, je veux que l'ensemble des utilisateurs du domaine puissent surfer au travers du proxy de manière authentifiée par Radius, dans le but de répondre besoin de traçabilité des accès vers internet et d'obtenir des logs légaux à présenter en cas d'enquête.

Tests d'acceptation :

Accès authentifié au proxy



Config du fichier /etc/squid/squid.conf

Account Name:	user1@secu23.internal
Account Domain:	SECU23
Fully Qualified Account Name:	secu23.internal/Users/User1
Client Machine:	
Security ID:	NULL SID
Account Name:	-
Fully Qualified Account Name:	-
Called Station Identifier:	-
Calling Station Identifier:	-
NAS:	
NAS IPv4 Address:	-
NAS IPv6 Address:	-
NAS Identifier:	Artica
NAS Port-Type:	Async
NAS Port:	111
RADIUS Client:	
Client Friendly Name:	Artica
Client IP Address:	192.168.100.10
Authentication Details:	
Connection Request Policy Name:	Use Windows authentication for all users
Network Policy Name:	Proxy
Authentication Provider:	Windows
Authentication Server:	SRV-PKI.secu23.internal
Authentication Type:	PAP

Log legaux

```
1701182095.731      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182095.734      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182095.736      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182095.738      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182095.740      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182095.743      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182141.346      0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.googletagmanager.com:443 - HIER_NONE/- text/html
1701182141.751      0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.googletagmanager.com:443 - HIER_NONE/- text/html
1701182142.824      0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.googletagmanager.com:443 - HIER_NONE/- text/html
1701182151.162  13206 192.168.23.100 TCP_TUNNEL/200 24957 CONNECT www.cpnv.ch:443 user1 HIER_DIRECT/128.65.195.179 -
1701182155.747      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182155.749      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182155.751      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182155.753      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182155.755      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1701182155.757      0 192.168.23.100 TCP_DENIED/403 4226 GET http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
```

Conclusion concernant l'authentification Radius du navigateur par le proxy